REMARKS

The claims are 1-34. Claims 1, 15, 30 and 32 have been amended. No new matter is introduced herein.

Claims 1-4, 6-17, 19, 21-34 stand rejected under 35 U.S.C. §102(b) as being anticipated by Burns et al; and claims 5 and 20 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Burns et al. in view of Johnson et al.; and finally claim 18 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Burns et al. in view of Roberts. These rejections are respectfully traversed as set forth in more detail below.

Claim 1 has been amended to further recite aspects of the claimed method to provide data security. In particular, claim 1 as amended further recites the features comprising:

providing at least one tag file, the tag file comprising a physical file of zero bytes in length;

maintaining the tag file in a part of a file system; and

processing file system calls so that the tag file appears as a secured file containing data from the view point of a user, operating system and programs.

Claim 1 as amended and now presented is as follows:

1. (currently amended) A method for providing data security in a device driver for accessing data, the method comprising the steps of:

providing at least one tag file, the tag file comprising a physical file of zero bytes in length;

maintaining the tag file in a part of a file system; and processing file system calls so that the tag file appears as a secured file containing

data from the view point of a user, operating system and programs, the method further comprising the steps of:

detecting a file system request;

completing said file system request;

receiving return information from said file system request;

determining whether said file system request is for a tag file associated with a secured file; and

if so, modifying said return information to reflect a file attribute of the secured file.

Applicant's claim 1 as set forth above is directed to the aspect of file spoofing in that from the viewpoint of a user, operating system and programs, a file that in actuality is zero bytes in length appears as a normal file containing data. However, the actual file containing the data is located in another part of the system, preferably in a secured area. It is respectfully submitted that this aspect set forth in Applicant's claim 1 is not seen to be taught or disclosed by Burns et al.

In view of the foregoing, Applicant respectfully solicits reconsideration and allowance of claim 1 together with claims 2-14 which are dependent either directly or indirectly from claim 1.

The remaining independent claims comprising claims 15, 30 and 32 have also been amended in a similar manner as claim 1, and for this reason, Applicant also solicits reconsideration and allowance of these independent claims together with the dependent claims 16-29, 31 and 33-34, which depend either directly or indirectly from claims 15, 30 and 32, respectively.

In view of all that is set forth above, Applicant respectfully solicits favorable consideration of this response and allowance of the present application.

Respectfully submitted,

Paul A. Taufer
Reg. No. 35,703

PAT:ers
215-656-3385